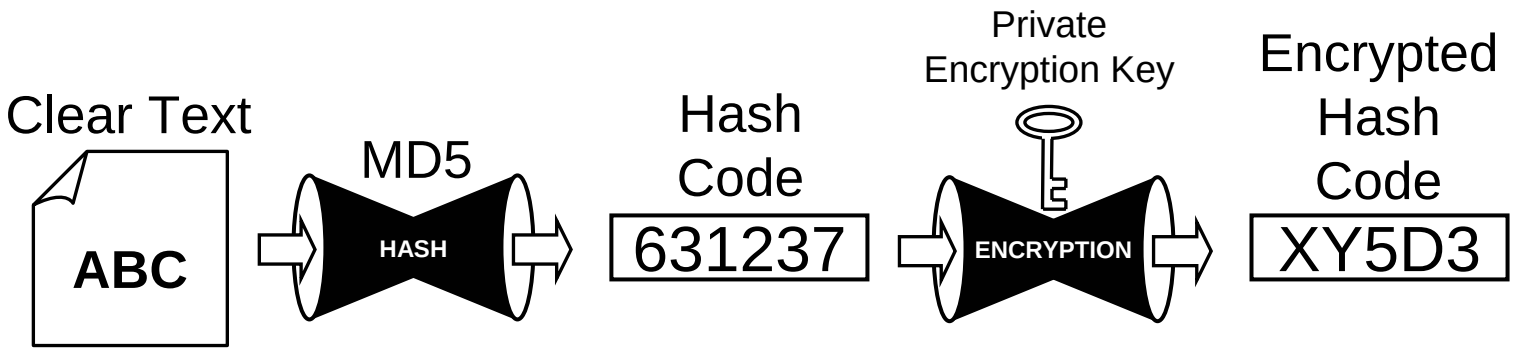
(The Sender)

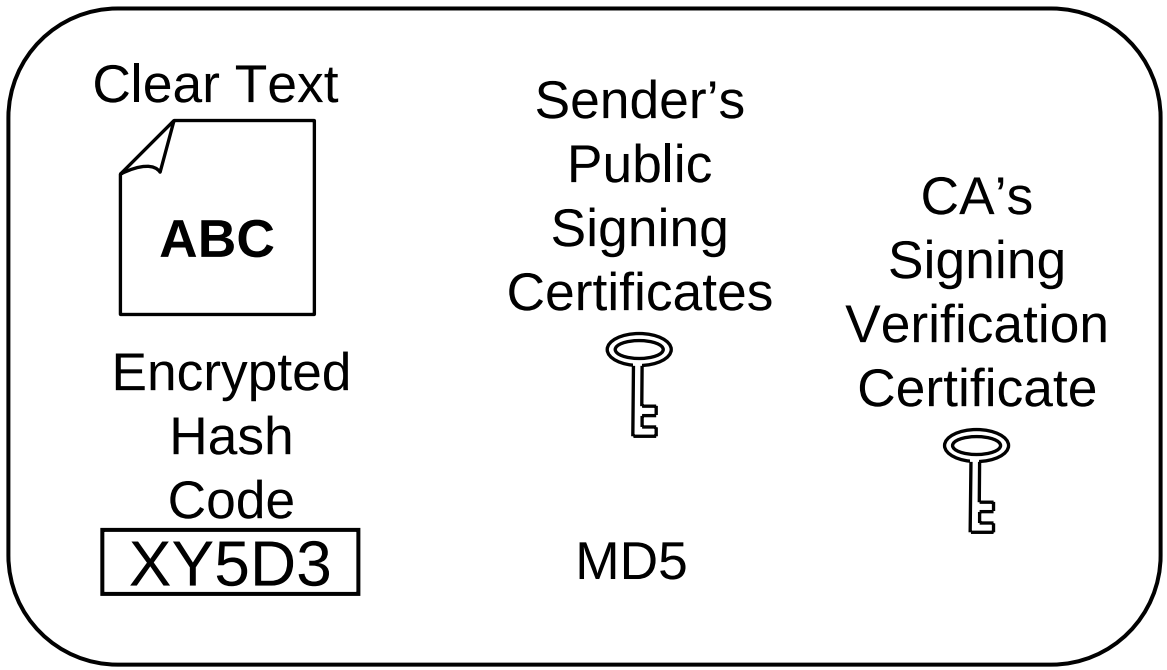
1. Create an encrypted hash code using the clear text message to be sent and the sender's private singing key



Signing keys:
- Public key is a decryption key (stored in a certificate)
- Private key is an encryption key

(The Sender)

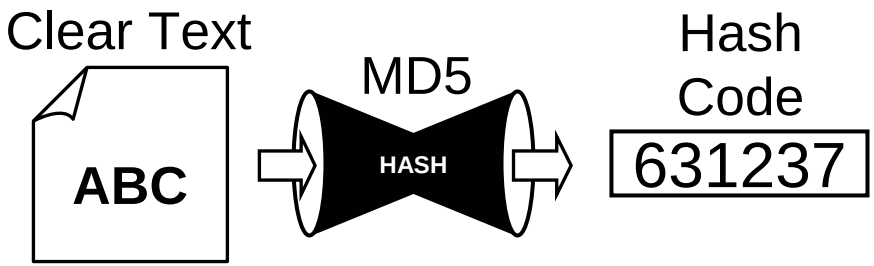
2 Package the clear text message, encrypted hash code, the name of the hash algorithm used, the sender's public signing certificate, the CA's signing verification certificate together and sent them to the recipient



(The Recipient)

1. Verify that the sender's signing certificate is valid

2. Create a hash code using the received hash code algorithm (name) and the received clear text message



(The Recipient)

3. Decrypt the received encrypted hash code using the sender's public signing key in the certificate

4. If the received and calculated hash codes match, the message was not modified in transit and was from the sender

Received Hash Code		Calculated Hash Code
631237	=	631237